UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/989,883	11/21/2001	Philippe Stransky	16674-6	1499

7590 09/21/2005

Clifford W. Browning
Woodard, Emhardt, Naughton, Moriarty & McNett
Bank One Center/Tower
111 Monument Circle, Suite 3700
Indianapolis, IN 46204-5137

EXAMINER	
SHIFERAW, ELENI A	
ART UNIT	**PAPER NUMBER**
2136	

DATE MAILED: 09/21/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/989,883	STRANSKY ET AL.	
	Examiner	Art Unit	
	Eleni A. Shiferaw	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 July 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☐ Claim(s) _____ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. Applicant's arguments with respect to claims 1-6 have been considered but are moot in view of the new ground(s) of rejection.

2. Claims 1-6 are presented for examination.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Holloway (Patent No.: US 6,424,718 B1) in view of Hardy et al. (Hardy, Patent No.: US 6,370,251 B1).

As per claim 1, Holloway teaches a method of production and distribution of asymmetric public and private keys between a key generation centre and at least one user unit (DEC), said unit comprising a security module (SM), said method consisting in:

generating certificates comprising a public key and a private key in a first cryptographic unit (KPG) (col. 8 lines 23-26),

coding the private key by means of a service key in the first cryptographic unit (KPG) and storing said private key in a key memory (KPS) (col. 8 lines 26-27),

when sending the keys to a user unit, extracting the keys from the key memory (KPS) (col. 3 lines 42-46, and col. 7 lines 31-36), composing the certification with the public key (col. 3 lines 52-59, and col. 9 lines 66-col. 10 lines 9),

decoding the corresponding private key by means of the service key in a cryptographic security module (col. 8 lines 66-col. 9 lines 1) and coding it with a transport key of the user (col. 4 lines 30-33, and col. 9 lines 66-col. 10 lines 9).

Holloway teaches encrypting the generated public/private key pairs. Holloway does not explicitly teach public/private keys are encrypted using the key generators secrete key as amended.

However Hardy discloses generating and storing key pairs at the key generation terminal, and encrypting the generated private key using key generation's terminal secrete key (access number/PIN) generated using secrete algorithm and terminal serial number (col. 2 lines 28-43).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Hardy within the system of Holloway because they are analogous in managing crypto keys. One would have been motivated to incorporate the teachings of encrypting the generated private key using the generators secrete key within the system of Holloway because it would enhance security. The generator's private key used to encrypt the key is private to the key generator. Enciphered and stored private keys are decrypted by generators key that is private to the generator only.

As per claim 2, Holloway and Hardy teach all the subject matter as described above. In addition, Holloway teaches a method, characterized in that the encrypted private key is received by the user unit (DEC) and transmitted to the security module (SM) containing the transport key for decoding and storing the private key (col. 7 lines 13-16 & 31-33, and col. 4 lines 48-51).

As per claim 3, Holloway and Hardy teach all the subject matter as described above. In addition, Holloway teaches a method, characterized in that it consists in using several monolithic cryptographic unit to obtain a high speed coding module (col. 9 lines 47-54 and abstract).

As per claims 4-6, Holloway and Hardy teach all the subject matter as described above. In addition, Holloway teaches a method, characterized in that it consists in:

coding the public key of the centre with the transport key and transmitting it to the user unit (DEC) (col. 8 lines 1-11 and lines 31-34),

receiving by the user unit, the encrypted public key and transmitting it to the security module (SM) (col. 9 lines 66-col. 10 lines 9, col. 8 lines 34-35, and col. 8 lines 66-col. 9 lines 1),

decoding and storing the public key by means of the transport key inside the security module (SM) (col. 9 lines 66-col. 10 lines 9, col. 8 lines 34-35, and col. 8 lines 66-col. 9 lines 1).

Conclusion

5. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A Shiferaw whose telephone number is 571-272-3867. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Eleni Shiferaw
September 19, 2005

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100